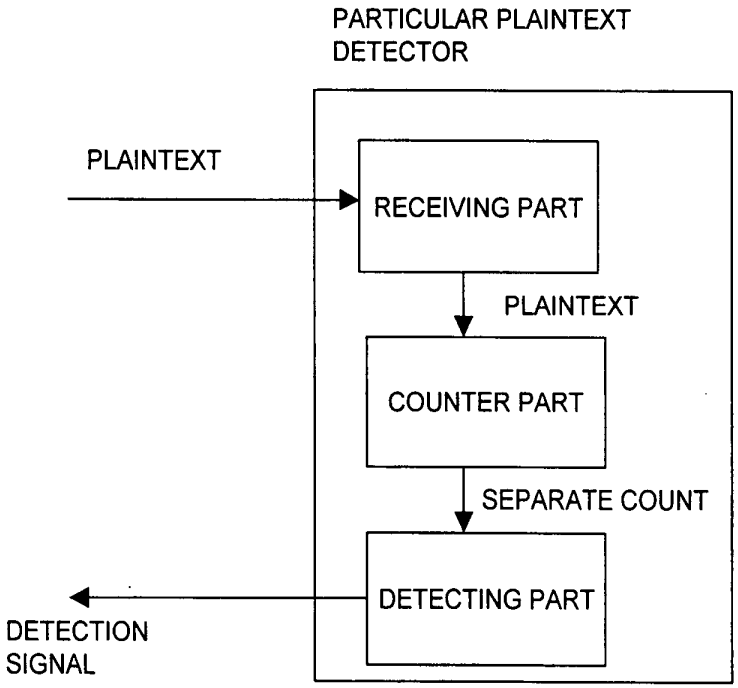

PARTICULAR PLAINTEXT
DETECTOR
PLAINTEXT
RECEIVING PART
PLAINTEXT
COUNTER PART
SEPARATE COUNT
DETECTING PART
DETECTION
SIGNAL

Fig.1

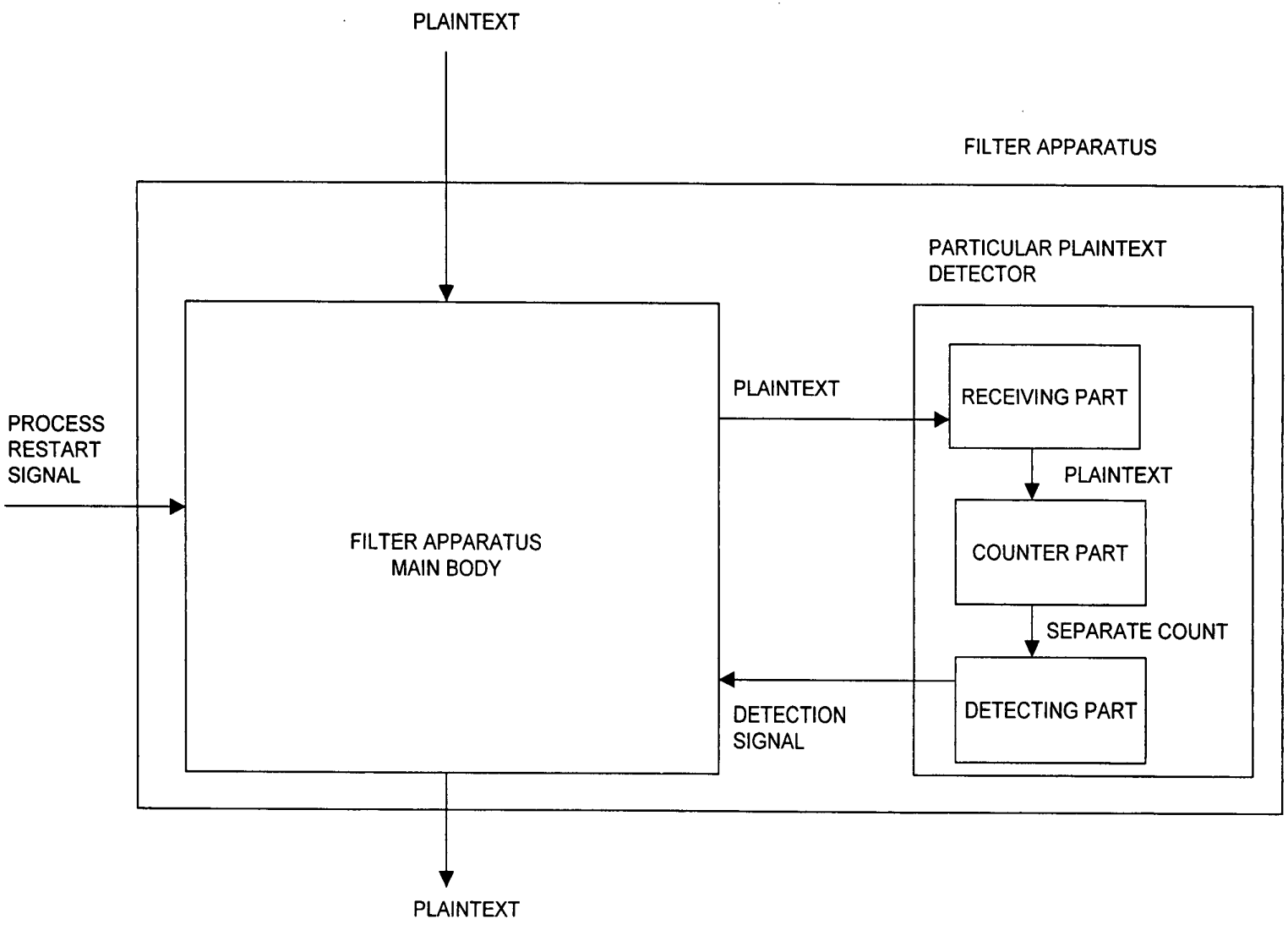

PLAINTEXT
FILTER APPARATUS
PARTICULAR PLAINTEXT DETECTOR
PROCESS RESTART SIGNAL
FILTER APPARATUS MAIN BODY
PLAINTEXT
RECEIVING PART
PLAINTEXT
COUNTER PART
SEPARATE COUNT
DETECTING PART
DETECTION SIGNAL
PLAINTEXT

Fig.2

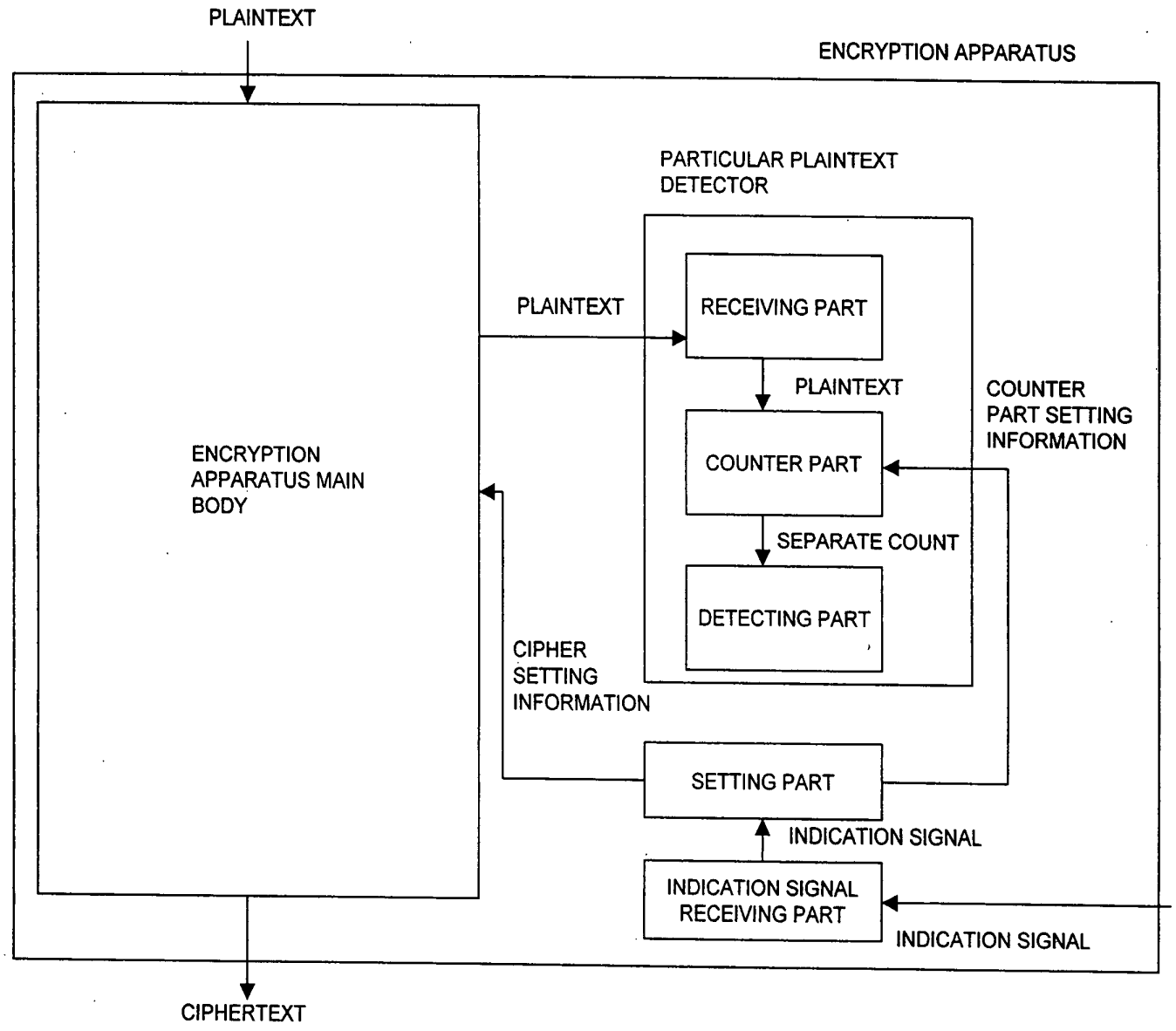

PLAINTEXT
ENCRYPTION APPARATUS
PARTICULAR PLAINTEXT DETECTOR
PLAINTEXT
RECEIVING PART
PLAINTEXT
COUNTER PART SETTING INFORMATION
ENCRYPTION APPARATUS MAIN BODY
COUNTER PART
SEPARATE COUNT
DETECTING PART
CIPHER SETTING INFORMATION
SETTING PART
INDICATION SIGNAL
INDICATION SIGNAL RECEIVING PART
INDICATION SIGNAL
CIPHERTEXT

Fig.3

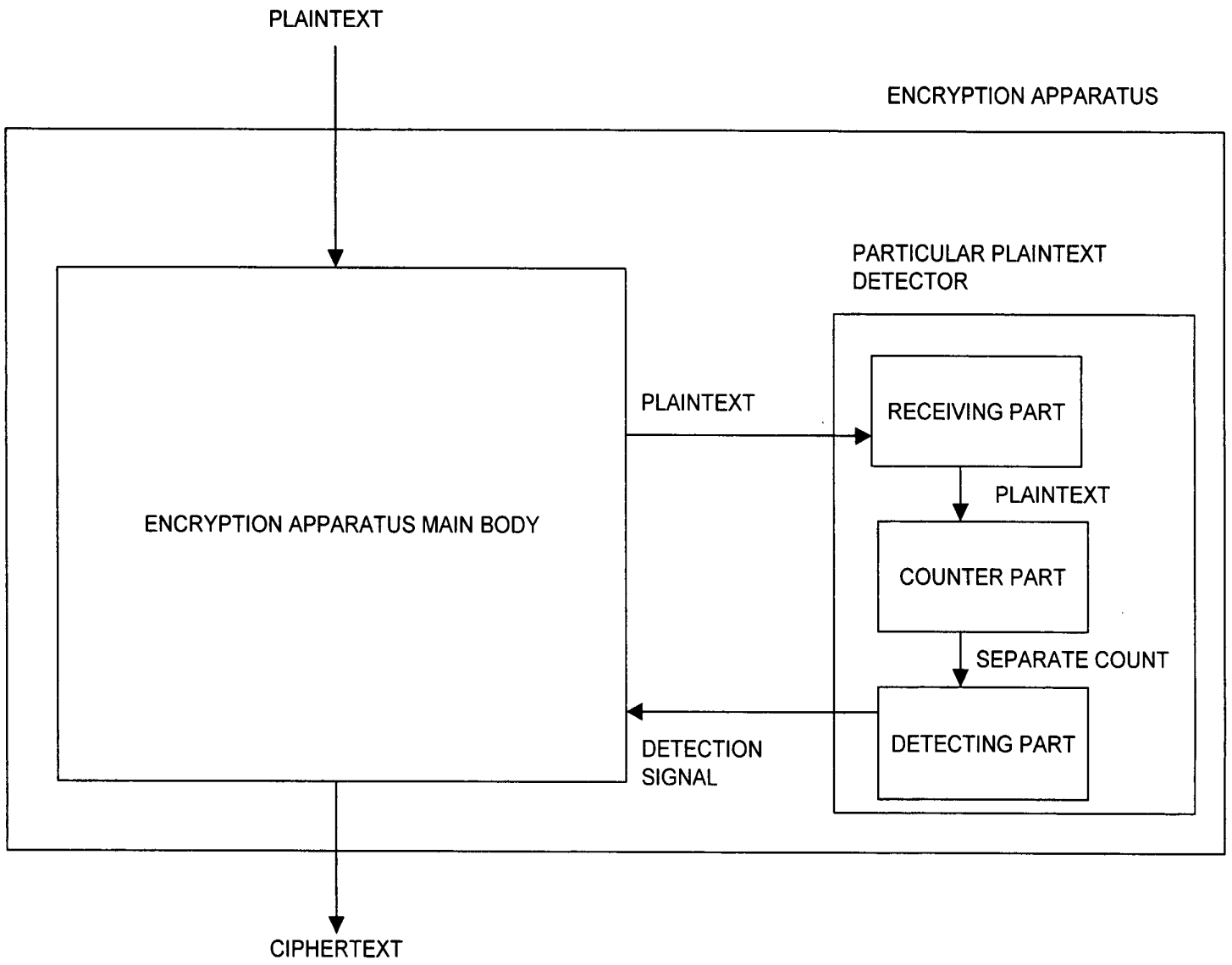

PLAINTEXT
ENCRYPTION APPARATUS
PARTICULAR PLAINTEXT DETECTOR
ENCRYPTION APPARATUS MAIN BODY
PLAINTEXT
RECEIVING PART
PLAINTEXT
COUNTER PART
SEPARATE COUNT
DETECTING PART
DETECTION SIGNAL
CIPHERTEXT

Fig.4

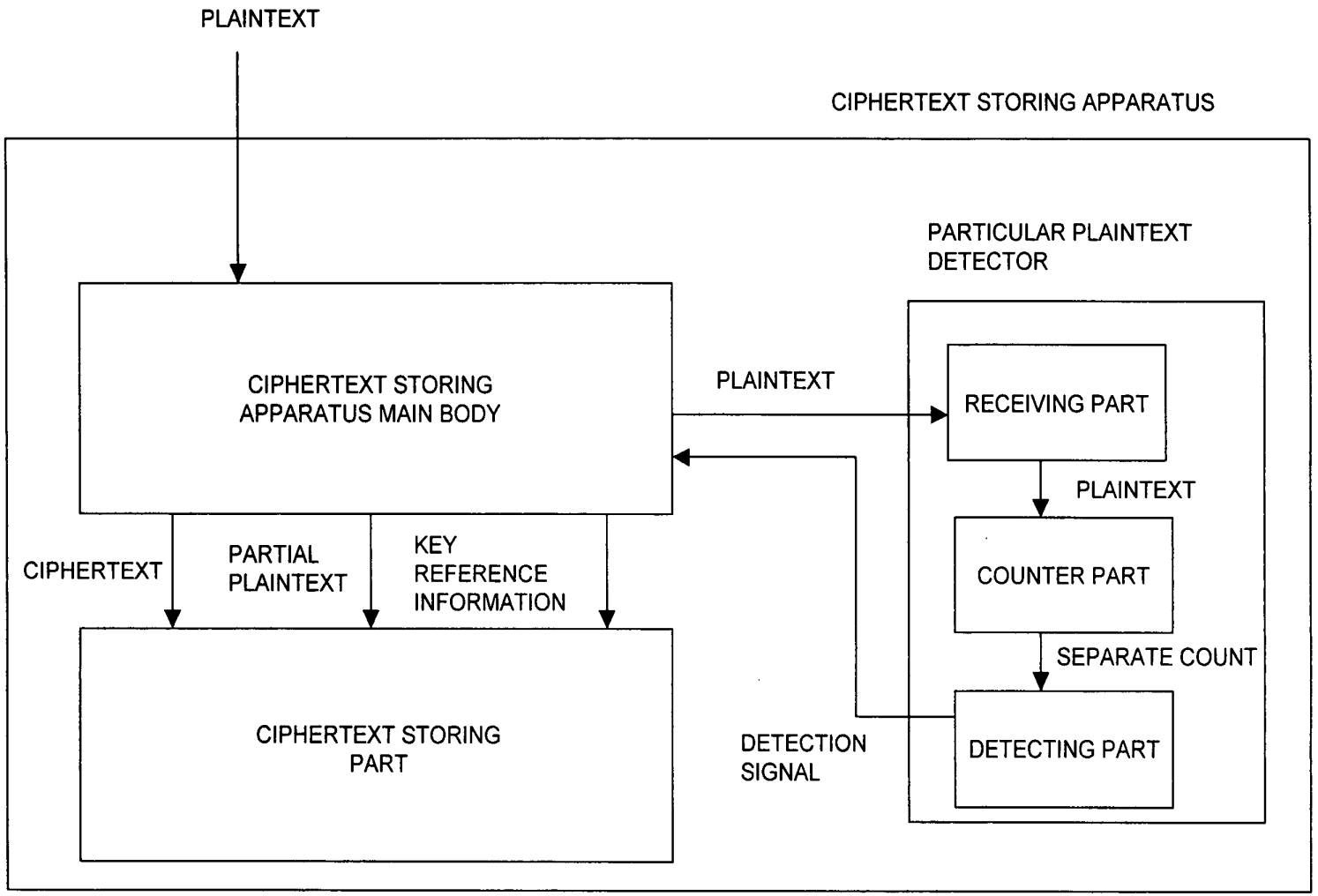

PLAINTEXT
CIPHERTEXT STORING APPARATUS
PARTICULAR PLAINTEXT DETECTOR
CIPHERTEXT STORING APPARATUS MAIN BODY
PLAINTEXT
RECEIVING PART
PLAINTEXT
COUNTER PART
SEPARATE COUNT
DETECTING PART
DETECTION SIGNAL
CIPHERTEXT
PARTIAL PLAINTEXT
KEY REFERENCE INFORMATION
CIPHERTEXT STORING PART

Fig.5

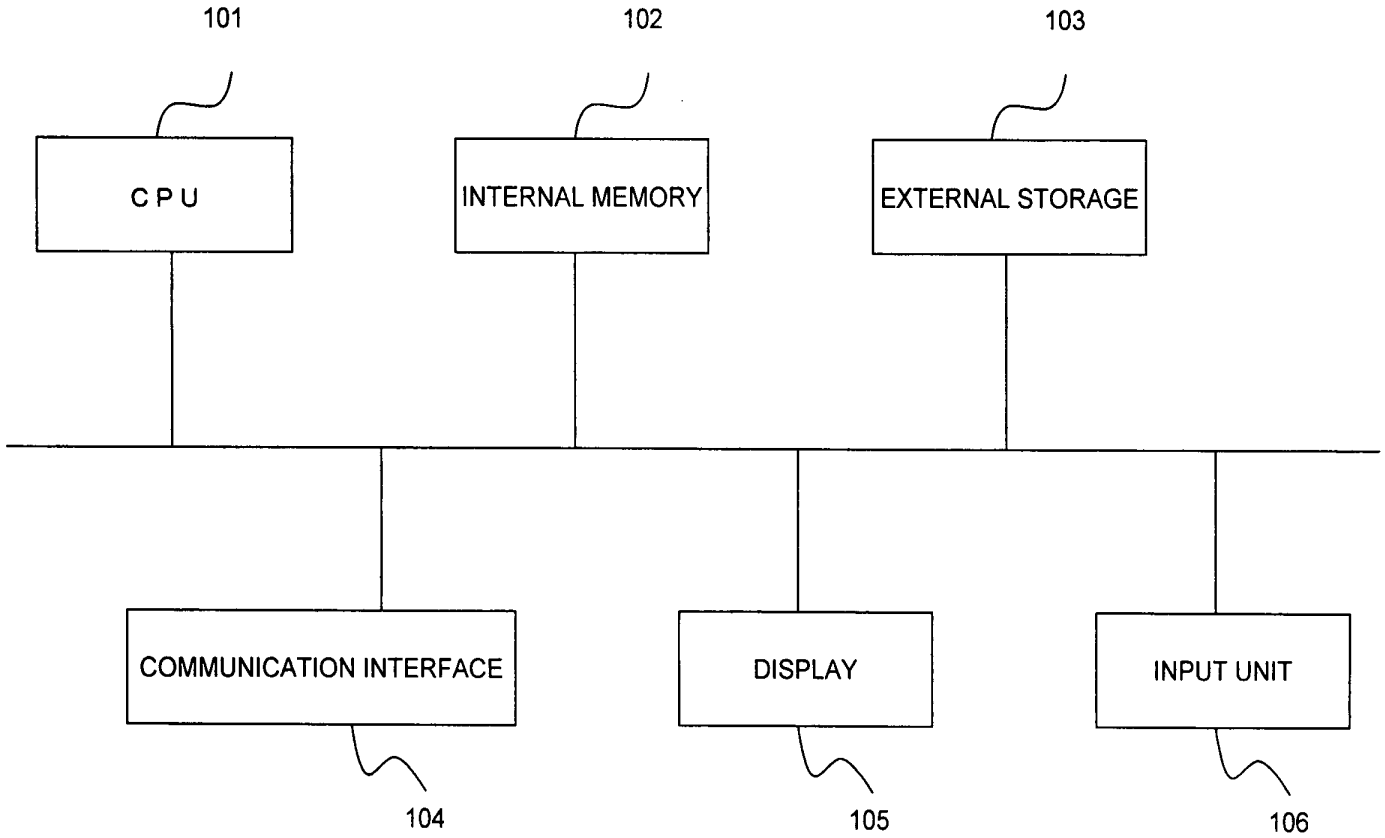

101
102
103
C P U
INTERNAL MEMORY
EXTERNAL STORAGE
COMMUNICATION INTERFACE
DISPLAY
INPUT UNIT
104
105
106

Fig.6

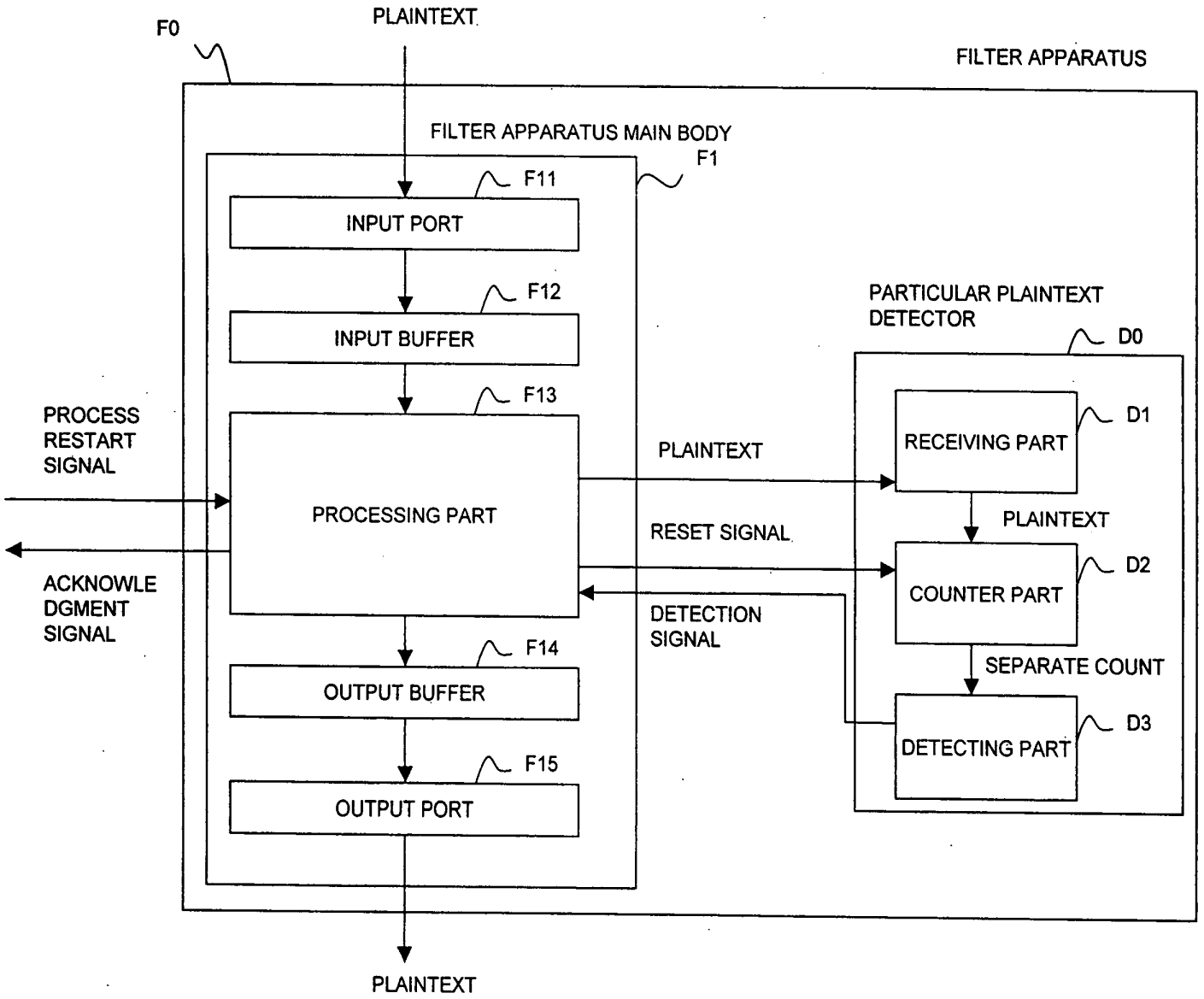

F0
PLAINTEXT
FILTER APPARATUS
FILTER APPARATUS MAIN BODY
F1
F11
INPUT PORT
F12
INPUT BUFFER
F13
PROCESSING PART
F14
OUTPUT BUFFER
F15
OUTPUT PORT
PLAINTEXT
PROCESS RESTART SIGNAL
ACKNOWLE DGMENT SIGNAL
PLAINTEXT
RESET SIGNAL
DETECTION SIGNAL
PARTICULAR PLAINTEXT DETECTOR
D0
RECEIVING PART
D1
PLAINTEXT
COUNTER PART
D2
SEPARATE COUNT
DETECTING PART
D3

Fig.7

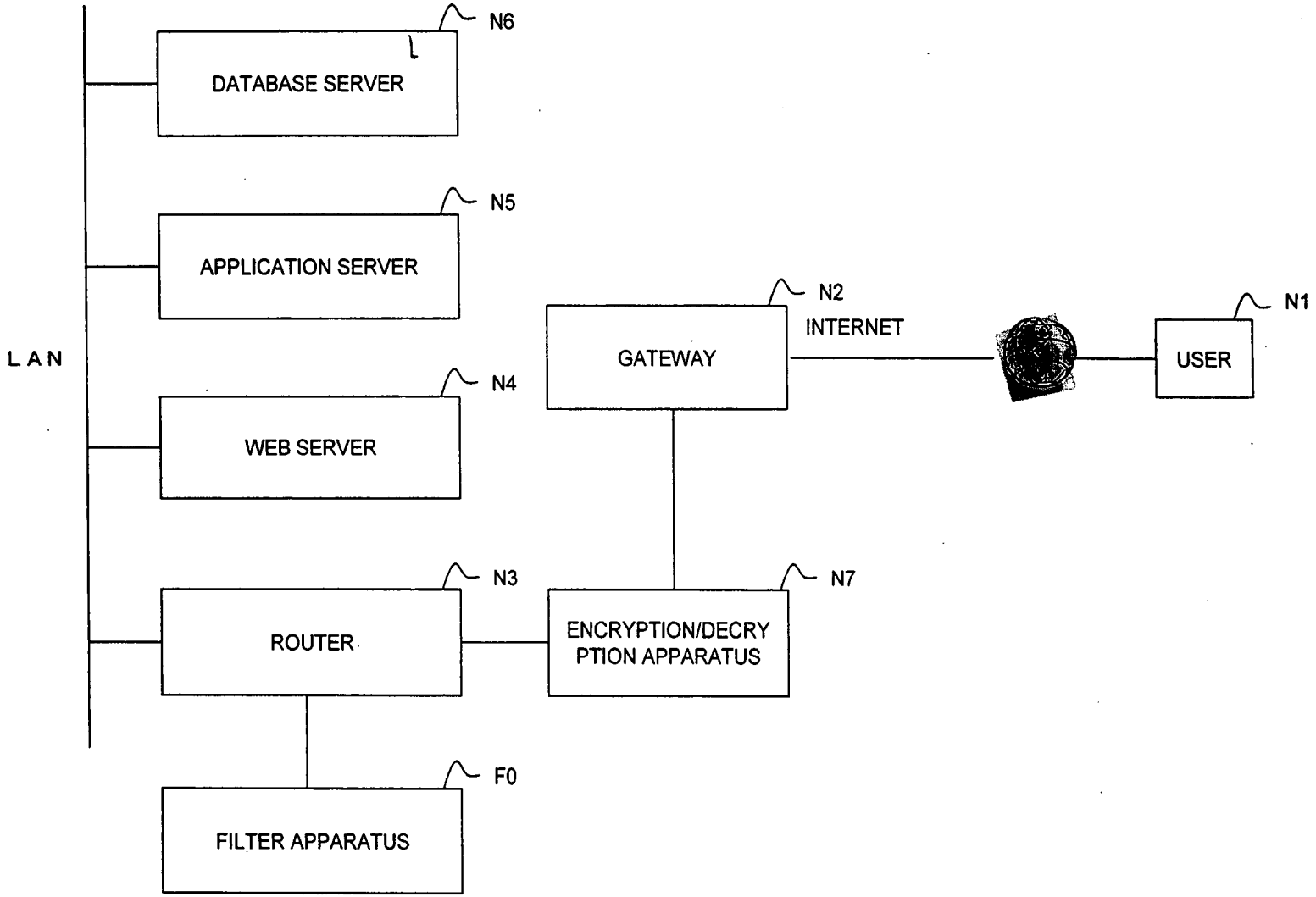

N6
DATABASE SERVER
N5
APPLICATION SERVER
N4
WEB SERVER
N3
ROUTER
F0
FILTER APPARATUS
LAN
N2
GATEWAY
INTERNET
N1
USER
N7
ENCRYPTION/DECRY
PTION APPARATUS

Fig.8

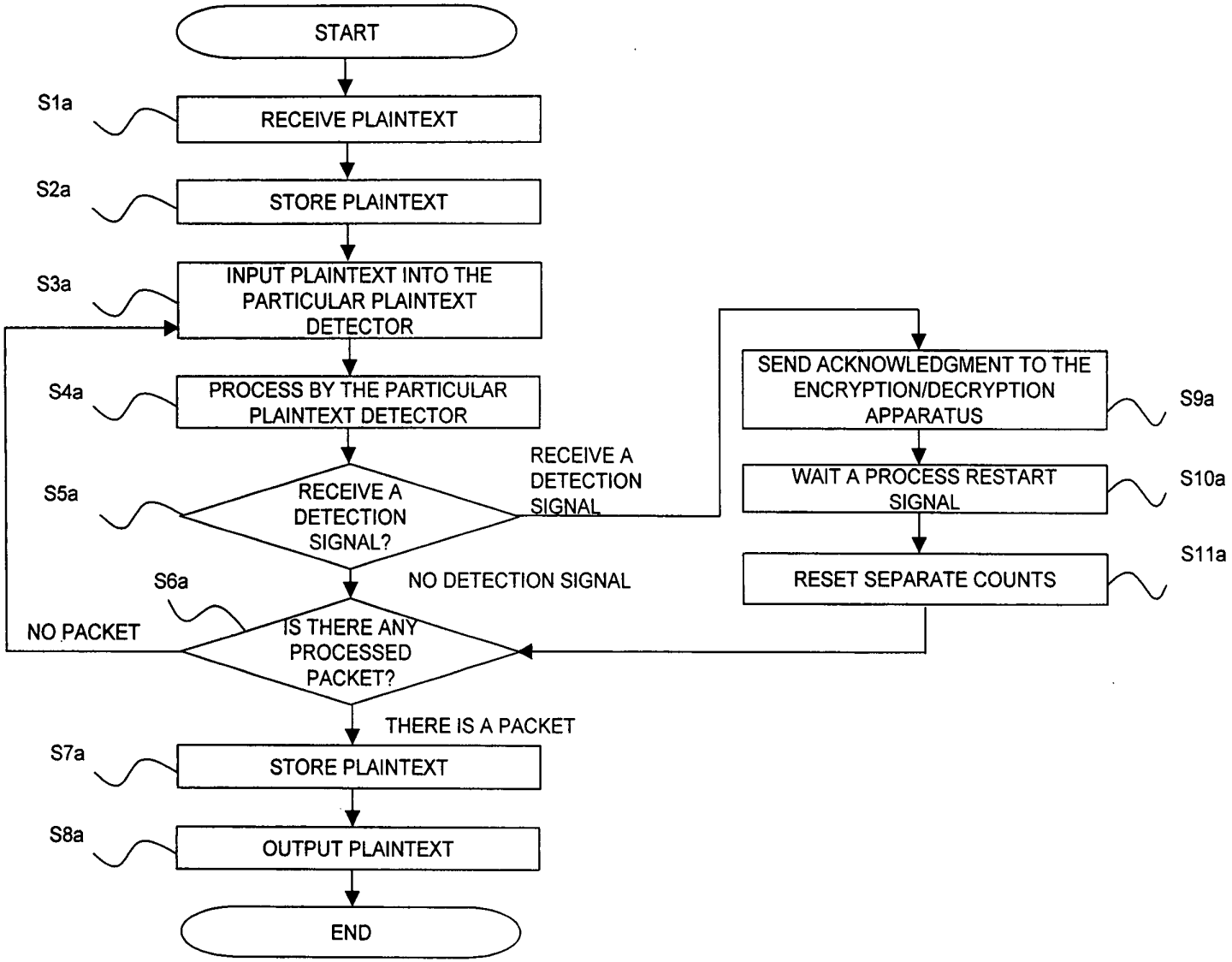

START
S1a
RECEIVE PLAINTEXT
S2a
STORE PLAINTEXT
S3a
INPUT PLAINTEXT INTO THE PARTICULAR PLAINTEXT DETECTOR
S4a
PROCESS BY THE PARTICULAR PLAINTEXT DETECTOR
S5a
RECEIVE A DETECTION SIGNAL?
RECEIVE A DETECTION SIGNAL
SEND ACKNOWLEDGMENT TO THE ENCRYPTION/DECRYPTION APPARATUS
S9a
WAIT A PROCESS RESTART SIGNAL
S10a
RESET SEPARATE COUNTS
S11a
NO DETECTION SIGNAL
S6a
IS THERE ANY PROCESSED PACKET?
NO PACKET
THERE IS A PACKET
S7a
STORE PLAINTEXT
S8a
OUTPUT PLAINTEXT
END

Fig.9

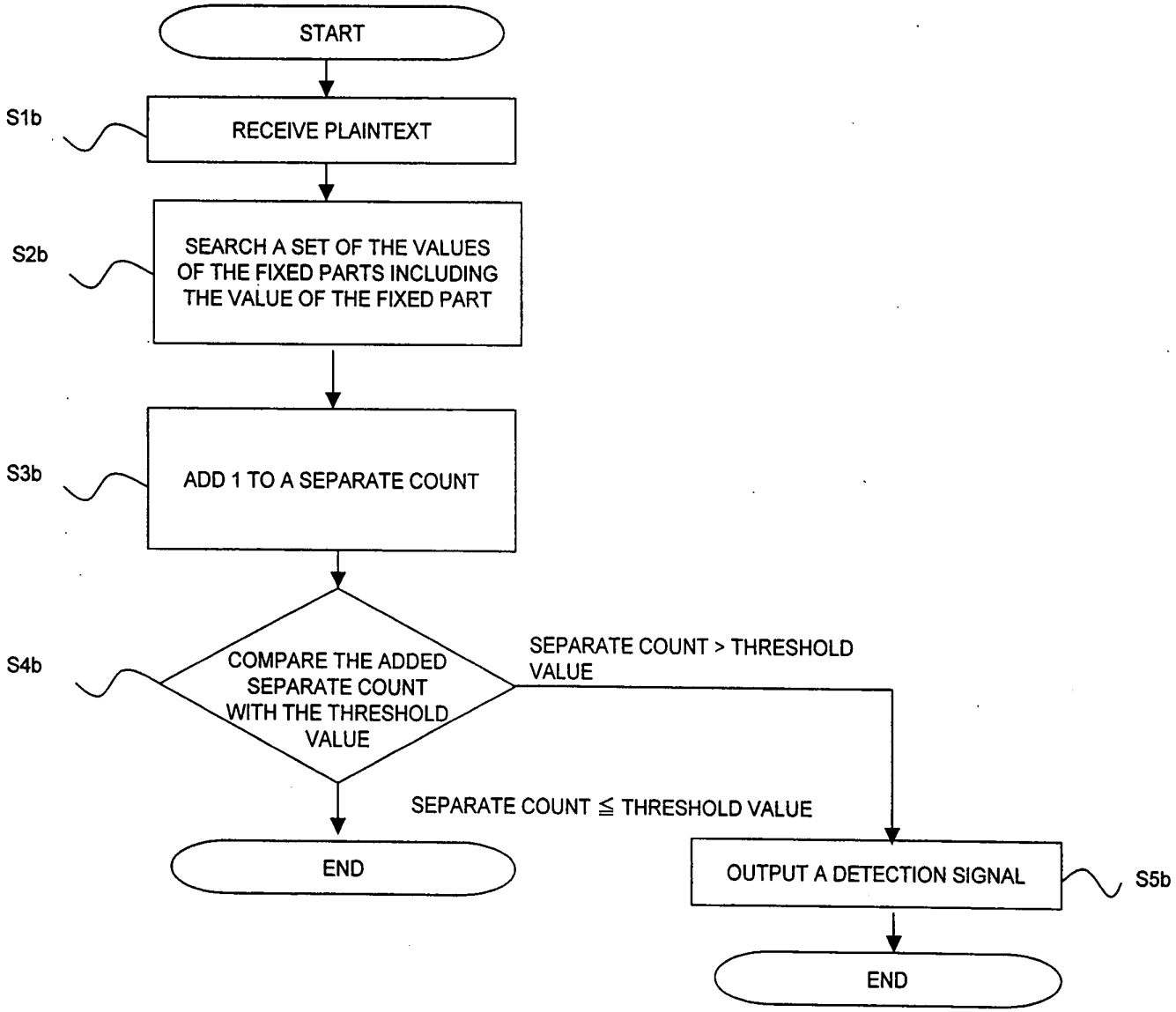

START
S1b
RECEIVE PLAINTEXT
S2b
SEARCH A SET OF THE VALUES OF THE FIXED PARTS INCLUDING THE VALUE OF THE FIXED PART
S3b
ADD 1 TO A SEPARATE COUNT
S4b
COMPARE THE ADDED SEPARATE COUNT WITH THE THRESHOLD VALUE
SEPARATE COUNT > THRESHOLD VALUE
SEPARATE COUNT ≦ THRESHOLD VALUE
END
OUTPUT A DETECTION SIGNAL
S5b
END

Fig.10

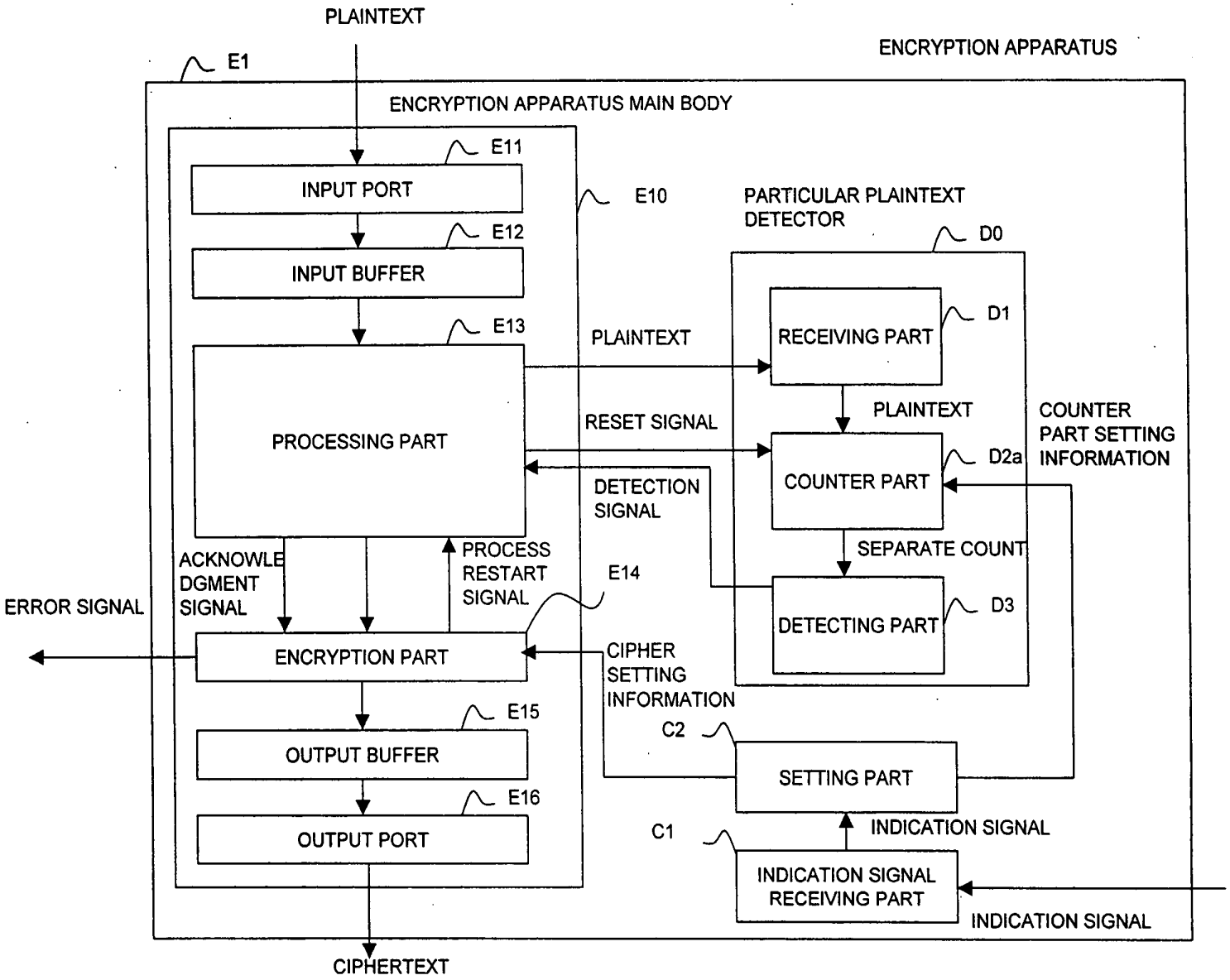

PLAINTEXT
E1
ENCRYPTION APPARATUS
ENCRYPTION APPARATUS MAIN BODY
E11
INPUT PORT
E10
PARTICULAR PLAINTEXT DETECTOR
D0
E12
INPUT BUFFER
E13
PLAINTEXT
RECEIVING PART
D1
PROCESSING PART
RESET SIGNAL
PLAINTEXT
COUNTER PART SETTING INFORMATION
COUNTER PART
D2a
DETECTION SIGNAL
ACKNOWLEDGMENT SIGNAL
PROCESS RESTART SIGNAL
E14
SEPARATE COUNT
ERROR SIGNAL
DETECTING PART
D3
ENCRYPTION PART
CIPHER SETTING INFORMATION
E15
C2
OUTPUT BUFFER
SETTING PART
E16
C1
INDICATION SIGNAL
OUTPUT PORT
INDICATION SIGNAL RECEIVING PART
INDICATION SIGNAL
CIPHERTEXT

Fig.11

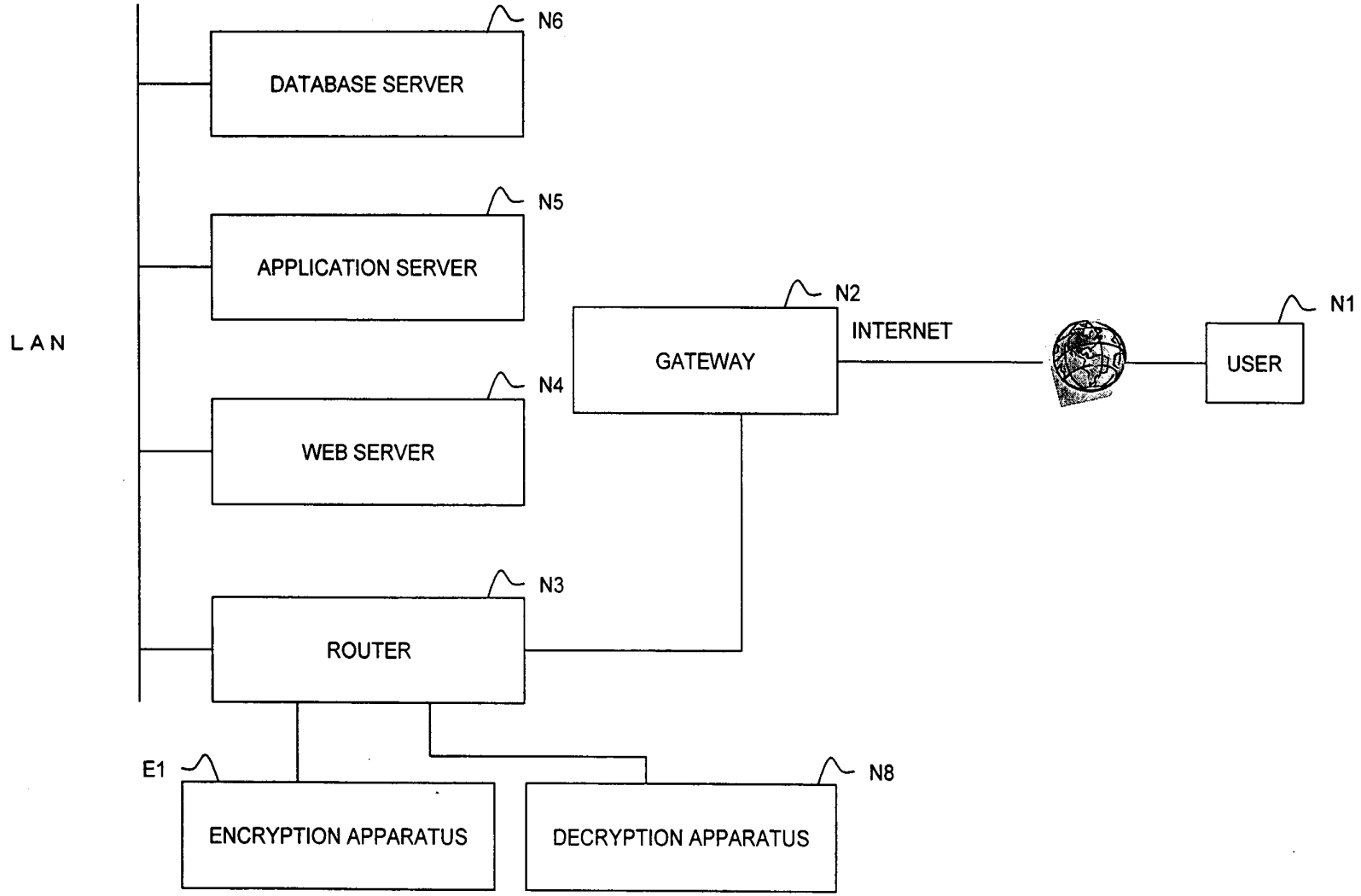

N6
DATABASE SERVER
N5
APPLICATION SERVER
N2
N1
INTERNET
L A N
GATEWAY
USER
N4
WEB SERVER
N3
ROUTER
E1
N8
ENCRYPTION APPARATUS
DECRYPTION APPARATUS

Fig.12

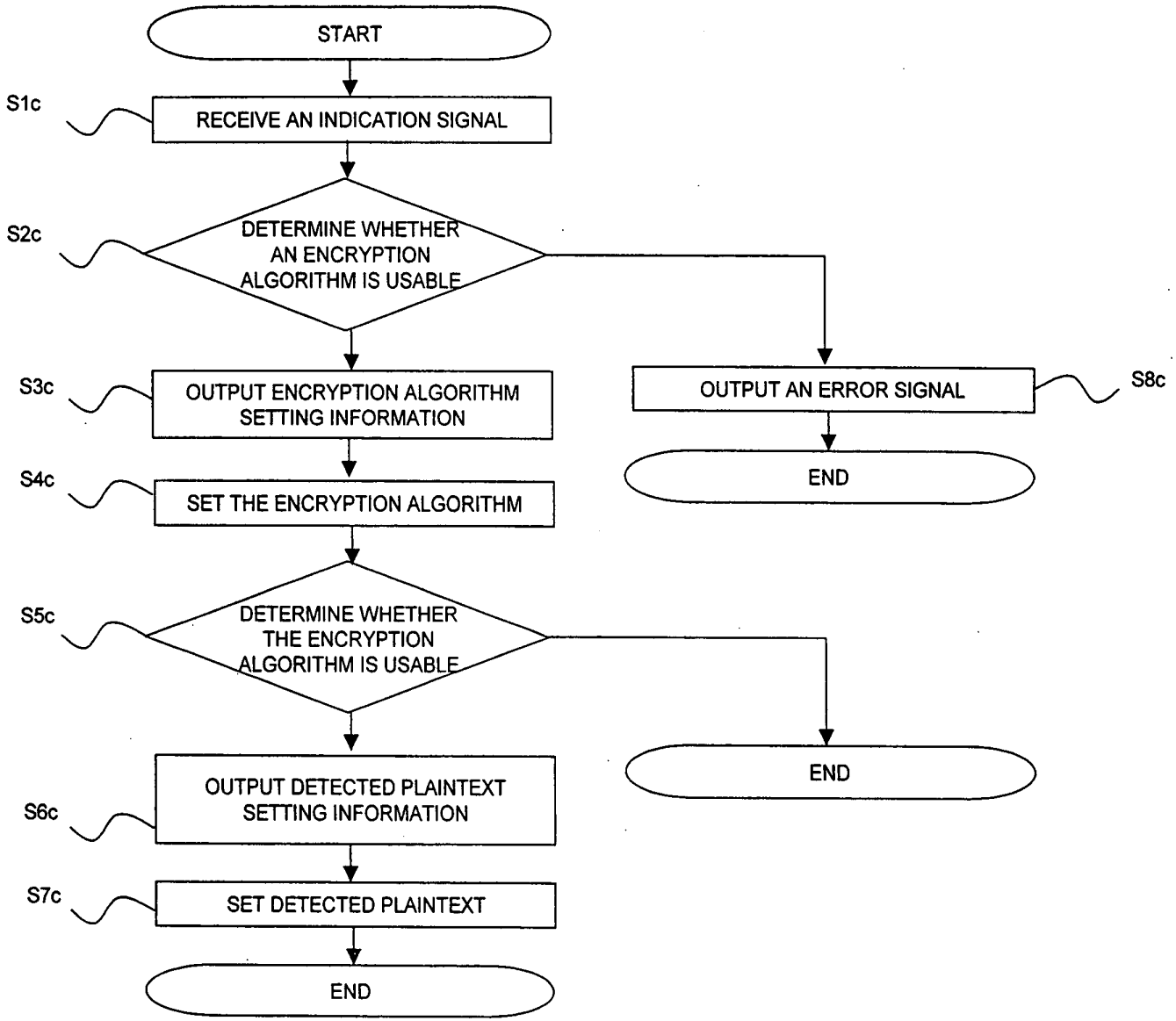
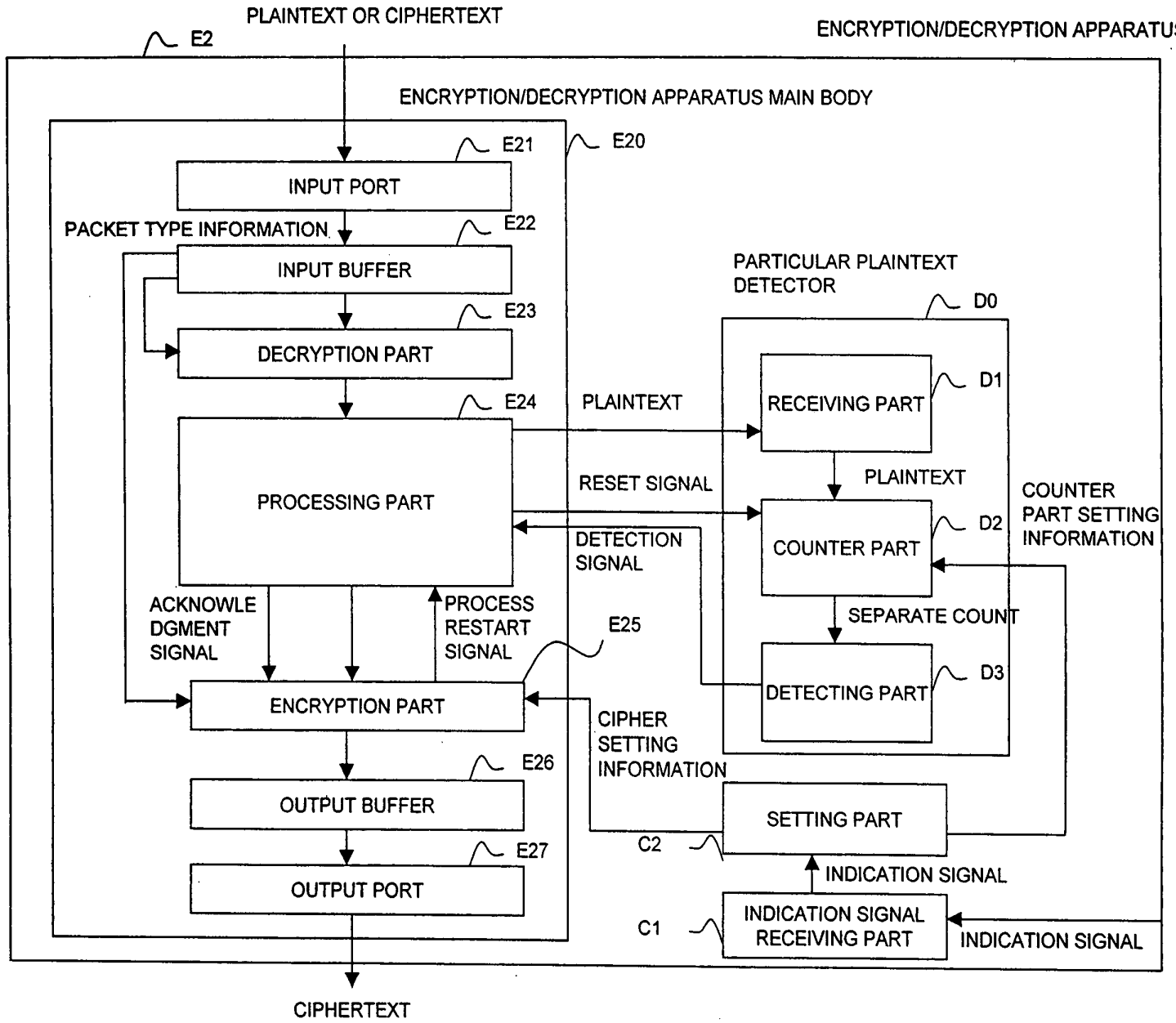

START
S1c
RECEIVE AN INDICATION SIGNAL
S2c
DETERMINE WHETHER AN ENCRYPTION ALGORITHM IS USABLE
S3c
OUTPUT ENCRYPTION ALGORITHM SETTING INFORMATION
S4c
SET THE ENCRYPTION ALGORITHM
S5c
DETERMINE WHETHER THE ENCRYPTION ALGORITHM IS USABLE
S6c
OUTPUT DETECTED PLAINTEXT SETTING INFORMATION
S7c
SET DETECTED PLAINTEXT
END
OUTPUT AN ERROR SIGNAL
S8c
END
END

Fig.13

Fig.14


PLAINTEXT OR CIPHERTEXT
E2
ENCRYPTION/DECRYPTION APPARATUS
ENCRYPTION/DECRYPTION APPARATUS MAIN BODY
E21
E20
INPUT PORT
PACKET TYPE INFORMATION
E22
INPUT BUFFER
E23
DECRYPTION PART
E24
PROCESSING PART
ACKNOWLE DGMENT SIGNAL
PROCESS RESTART SIGNAL
E25
ENCRYPTION PART
E26
OUTPUT BUFFER
E27
OUTPUT PORT
CIPHERTEXT
PARTICULAR PLAINTEXT DETECTOR
D0
PLAINTEXT
RECEIVING PART
D1
PLAINTEXT
RESET SIGNAL
COUNTER PART
D2
COUNTER PART SETTING INFORMATION
DETECTION SIGNAL
SEPARATE COUNT
DETECTING PART
D3
CIPHER SETTING INFORMATION
SETTING PART
C2
INDICATION SIGNAL
C1
INDICATION SIGNAL RECEIVING PART
INDICATION SIGNAL

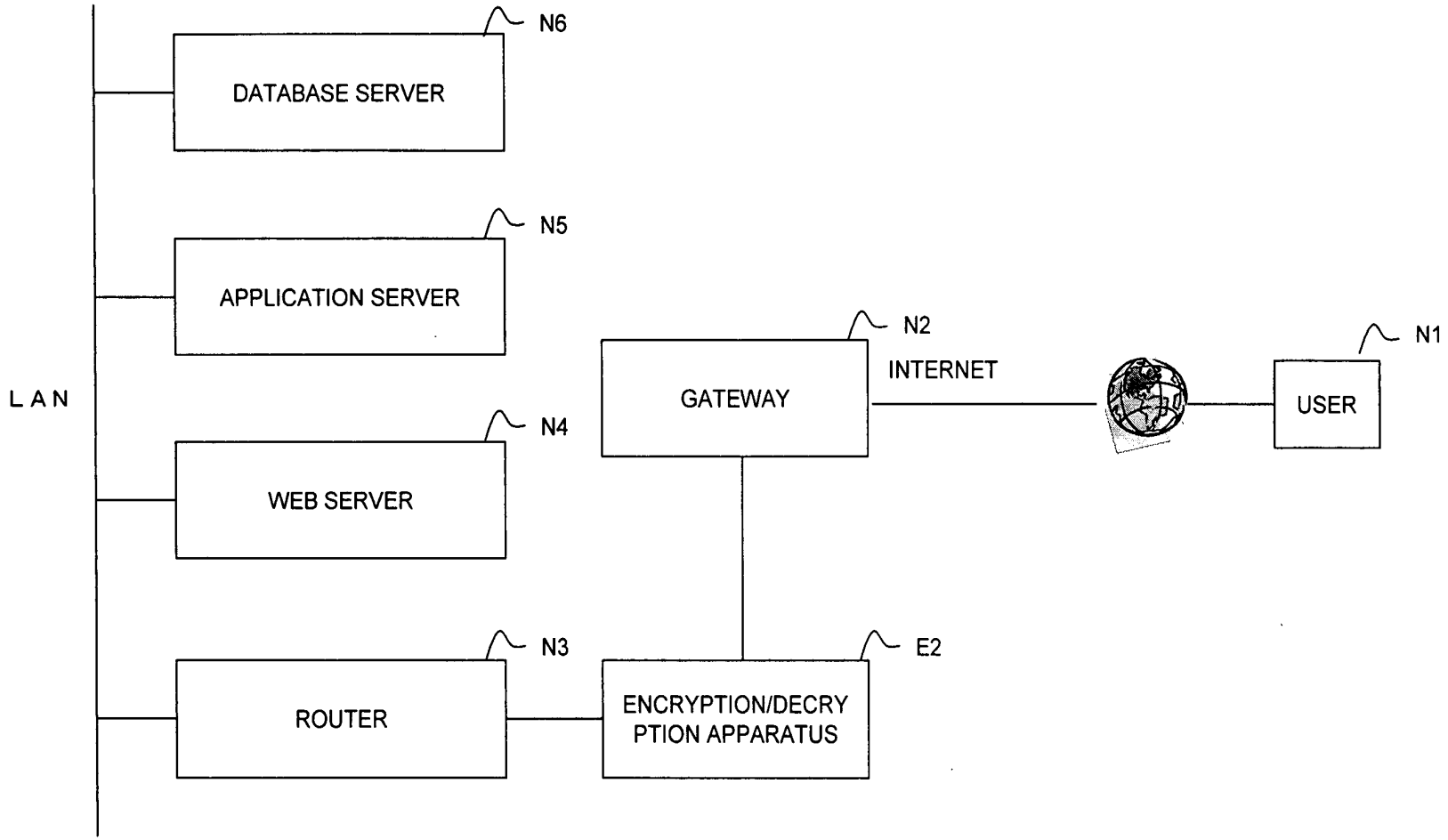
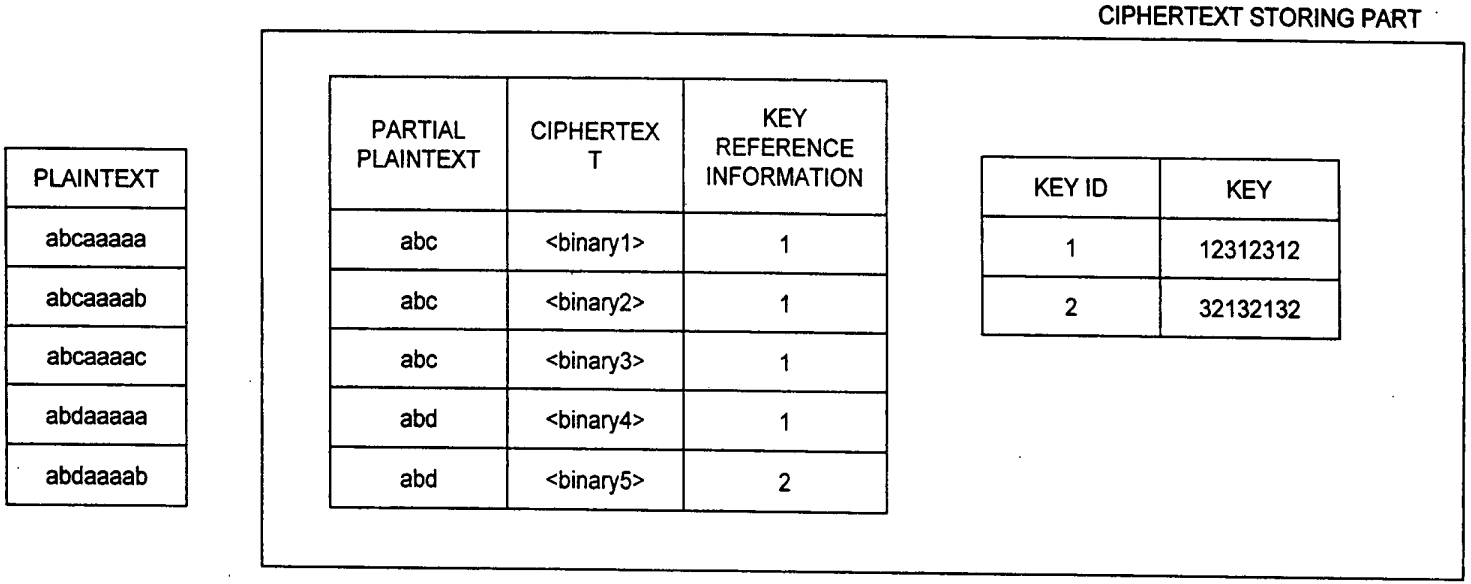

N6
DATABASE SERVER
N5
APPLICATION SERVER
N4
WEB SERVER
N3
ROUTER
L A N
N2
GATEWAY
INTERNET
N1
USER
E2
ENCRYPTION/DECRY
PTION APPARATUS

Fig.15



<binary1> = Enc(abcaaaaa)

<binary2> = Enc(abcaaaab)

<binary3> = Enc(abcaaaac)

<binary4> = Enc(abdaaaaa)

<binary5> = Enc(abdaaaab)

Enc() INDICATES ENCRYPTION PROCESS

CIPHERTEXT = Enc(PLAINTEXT)

Fig.16